

ORIGINAL

United States District Court

SOUTHERN DISTRICT OF INDIANA

UNITED STATES OF AMERICA

V.

CRIMINAL COMPLAINT

KEVIN M. STEWART

CASE NUMBER: 1:08-mj-0238

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about July 23, 2008 to September 30, 2008 in Marion County, in the Southern District of Indiana defendant did, (Track Statutory Language of Offense)

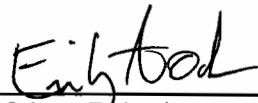
Count 1: Use interstate communications with intent to extort and threat an individual or company

Count 2: Fraud and Related Activity in Connection with Computers

in violation of Title 18, United States Code, Sections 875 and 1030(a)(7)(B) and (C). I further state that I am a Special Agent and that this complaint is based on the following facts:

See attached Affidavit

Continued on the attached sheet and made a part hereof.



Emily Odom, Federal Bureau of Investigations

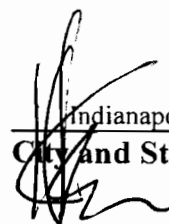
Sworn to before me, and subscribed in my presence

October 1, 2008
Date

Kennard P. Foster, U.S. Magistrate Judge
Name and Title of Judicial Officer

at Indianapolis, Indiana

City and State



Signature of Judicial Officer

AFFIDAVIT

I, Emily A. Odom, having been duly sworn according to law, depose and state as follows:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed since June 25, 2006. I am assigned to the Cyber Squad and have received training in conducting Cyber investigations. Before joining the FBI, I earned a Masters of Science degree, majoring in Computer and Information Science. I worked professionally as a Systems Analyst for approximately two years and a software developer for approximately four years.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

APPLICABLE STATUTES

3. Title 18 U.S.C. § 875 (Interstate Communications) states that whoever, with intent to extort from any person, firm, association or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years or both.

4. Title 18 U.S.C. § 1030(a)(7) (Fraud and Related Activity in Connection with Computers) makes it a federal crime for a person, with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any . . . (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion. As described herein, 18 U.S.C. § 1030(a)(7)(B) and (C) became effective on September 26, 2008. *See* HR 5938 (which became PL 110-326, 122 Stat. 3560).

BACKGROUND

5. On March 31, 2006, Medical Excess, a member company of American International Group (AIG), was the victim of a burglary at their office in Indianapolis, Indiana. Medical Excess operates as a specialty medical underwriter which focuses on catastrophic medical risk management.

6. The items stolen during the burglary included a computer server that was contained in a locked room. The stolen server contained the names of over 900,000 insured persons; including, in many cases, their personally identifying information and their confidential medical information. The server also contained confidential internal e-mail communications.

7. The Marion County Sheriff's Department, with assistance from the FBI, conducted an investigation into this matter, but did not identify a subject. Because of additional further leads, the FBI closed its investigation on August 22, 2007.

8. On the morning of July 23, 2008, an unidentified white male entered the office building containing the Medical Excess office suite and pushed a letter-sized manilla envelope under the unmarked rear door of the Medical Excess suite. The envelope was addressed, "For the person in charge of this AIG Midwest Office." The contents of the envelope included a letter, spreadsheet printouts, and a CD-ROM.

9. The letter informed AIG/Medical Excess that the sender, hereinafter referred to as the unknown subject (UNSUB), was in possession of the stolen server and its sensitive contents.

The UNSUB demanded that AIG pay the UNSUB \$1,000 each week for four years, totaling \$208,000. The letter stated that if the payments were made, the personal identifying information and medical information would not be released. If payments were not made, the UNSUB threatened to release the data onto the Internet. The UNSUB demanded that the money be paid into WebMoney account XXXXXXXXXX9318 utilizing WMZ e-currency at the Internet web site wmtransfer.com. The UNSUB also stated that AIG could contact the UNSUB through the email address aigmidwest@safe-mail.com.

10. On July 25, 2008, SA Michael Alford accessed the CD noted above and retrieved its contents. Representatives of AIG verified that the data on the CD, as well as the spreadsheet printouts contained in the delivered envelope, were a sample of the data contained on the server that was stolen in 2006.

11. Research by SA Robert Herzog identified Webmoney as an electronic currency and online payment system, which was founded by WM Transfer Ltd., and located in Moscow, Russia. WebMoney transactions are conducted through Webmoney Transfer which can be accessed at the Internet website wmtransfer.com. SA Herzog determined that, as with other online payment services, money can be moved from one person to another through the WebMoney service.

12. On July 25, 2008 Task Force Officer (TFO) Bernard L. Durham identified cameras on a building adjacent to the building which contains the Medical Excess office suite. The building was then identified as the Kappa Alpha Theta Fraternity. TFO Durham contacted the Assistant Director of Administration, KATF, 8740 Founders Road, Indianapolis, Indiana, to review the surveillance videos. After reviewing the videos TFO Durham identified what appeared to be the UNSUB arriving in a red coupe, parking in the KATF parking lot, and

walking towards the Medical Excess building. Approximately five minutes later, the individual returned to the car and drove away.

13. Also, on July 25, 2008, SA Herzog registered the email account mcsteve55@gmail.com for use by a Medical Excess company representative to communicate with the UNSUB at email address aigmidwest@safe-mail.com.

14. On July 29, 2008, a representative of Medical Excess, with assistance from SA Herzog, established a WebMoney account to deposit and transfer money to the UNSUB. During the account registration process, SA Herzog was required to provide a valid e-mail address and mobile phone number to receive a verification e-mail and text message.

15. On July 30, 2008, at 12:13 p.m. EDT, an email was received from aigmidwest@safe-mail.com that was addressed to mcsteve55@gmail.com. Analysis of the email header information revealed the email was sent from IP address 75.145.149.150. A Federal Grand Jury Subpoena was subsequently sent to Comcast Cable Communications requesting the subscriber to the IP address on the date and time the email was received. On August 11, 2008, Comcast Cable Communications replied via facsimile listing the subscriber to the IP address as the Lodge At Trail Apartments, 9541 Benchview Drive, Indianapolis, Indiana 46240.

16. On July 31, 2008, at 9:48 a.m. EDT, an email was received from aigmidwest@safe-mail.com which was addressed to mcsteve55@gmail.com. Analysis of the email header information revealed the email was sent from IP address 68.58.2.237. A Federal Grand Jury Subpoena was subsequently sent to Comcast Cable Communications requesting the subscriber to the IP address on the date and time the email was received. On July 31, 2008, Comcast Cable Communications replied listing the subscriber to the IP address as PERSON 1, 925 Carlyle Lane, Unit D, Indianapolis, Indiana 46240.

17. On August 4, 2008 at 12:44 p.m. EDT, an email was received from aigmidwest@safe-mail.com which was addressed to mcsteve55@gmail.com. Analysis of the email header information revealed the email was sent from IP address 68.58.115.198. A Federal Grand Jury Subpoena was subsequently sent to Comcast Cable Communications requesting the subscriber to the IP address on the date and time the email was received. On August 21, 2008, Comcast Cable Communications replied listing the subscriber to the IP address as PERSON 1, 1004 Carlyle Lane, #C, Indianapolis, Indiana 46240.

18. On August 6, 2008, a representative of Medical Excess, with assistance from SA Herzog, made an initial payment of \$1,500 into the UNSUB's WebMoney account. Through the transaction process, the WebMoney site displayed the UNSUB's account "alias" as "jeheardl," WebMoney Identification (WMID) number as XXXXXXXXX6057, with a creation date of July 17, 2008.

19. On or about August 6, 2008, SA Herzog, through FBI Headquarters and the FBI Legal Attache (LEGAT) in Moscow, made a request to the Russian Ministry of Internal Affairs to obtain subscriber information from WM Transfer, Ltd. regarding the WebMoney user "jeheardl" and WMID XXXXXXXXX66057.

20. On August 12, 2008, Supervisory Special Agent (SSA) Steven Bongardt provided to SA Odom a spreadsheet he received via email from the Indiana State Police which contained the results of a search of red two-door coupe and hatchback vehicles on record in the 46240 zip code. The spreadsheet included approximately 84 vehicles. Included in this list was a red two-door 2004 Chevrolet Cavalier registered to Kevin M. Stewart, 9133 Chesterbrook Court. The apartment number was missing from this record. SA Odom reviewed this address and

determined it to be in the immediate vicinity of the addresses identified in paragraphs 15, 16, 17 as being Internet accounts from which communications from the UNSUB originated.

21. On September 15, 2008, SA Herzog received an e-mail communication from LEGAT Moscow that the Russian Ministry of Internal Affairs had fulfilled the request for information and provided the subscriber information for Webmoney user account "jeheard" and WMID XXXXXXXXX6057 as follows:

Project Name, Web Name:	jeheard
Last Name:	Jeff
First Name:	Hearld
E-mail:	jeheard@gmail.com
Telephone Number:	317.223.2871
City/Country:	New York/United States of America
Address:	jeheard@gmail.com

22. On September 10, 2008, Steven Tursi, Director of Global Investigations of American International Group, provided via email a document to SA Odom listing the subscriber information for WMID XXXXXXXXX66057 that he obtained by way of his corporate investigation. The subscriber information was listed as follows:

Project Name, Web Name:	jeheard
Last Name:	Jeff
First Name:	Hearld
E-mail:	jeheard@gmail.com
Telephone Number:	317.223.2871
City/Country:	New York/United States of America
Address:	jeheard@gmail.com

23. In addition to the subscriber information provide by Tursi was transactional history related to WMID XXXXXXXXX6057, to include login time, logoff time and IP address information for access to the WMID. Among the records was access to the WMID on August 6, 2008 form IP address 68.57.200.159 at the following login and logoff times in MSD (Moscow Daylight Time).

Login at 02:41 and logoff at 02:42

Login at 02:43 and logoff at 02:45

Login at 03:00 and logoff at 03:01

24. On September 16, 2008, a subpoena was sent to Comcast requesting subscriber information for IP address 68.57.200.159 and on September 23, 2008 Comcast replied with the following information:

Subscriber Name:	Jordan YMCA
Service Address:	8400 Westfield Road Indianapolis, Indiana 46240

25. On September 25, 2008, TFO Joel Arthur received via email the Jordan Branch YMCA scan access report for August 5, 2008 from Aaron Bobinskey, Business Service Director of the Jordan Branch YMCA. This report contained a list of YMCA members that entered the facility on that day, thus having their membership card scanned at the front desk. The report listed the YMCA Branch, last name, preferred name, and scan time of all individuals entering the YMCA. Also, on September 25, 2008, TFO Arthur obtained surveillance video from the Jordan Branch YMCA for August 5, 2008.

26. On September 29, 2008, SA Odom reviewed the scan access report and determined that a Kevin Stewart swiped into the Jordan Branch YMCA on August 5, 2008 at 6:28 p.m. SA Odom then reviewed the video surveillance obtained by TFO Arthur and identified a white male matching the description of the UNSUB entering the YMCA at 6:28 p.m. The white male entered the YMCA carrying what appeared to be a laptop computer bag over his right shoulder. He exited the YMCA at approximately 7:45 p.m.

27. On September 29, 2008, TFO Brian Bethel conducted a search of the Indianapolis Metropolitan Police Department database and discovered a police report made on September 2,

2006 in which a Kevin M. Stewart was a witness of a crime. In the report Stewart stated he was an employee of Eagle Trident Security.

28. On September 29, 2008, SA Odom contacted Steven Tursi and inquired as to who handled the building security for 8777 Purdue Road, Indianapolis, Indiana. Tursi informed SA Odom the security company for the building was currently Eagle Trident Security and that they were the security company over the building during the initial 2006 burglary.

29. On September 30, 2008, surveillance was initiated on Kevin M. Stewart at his residence, 9133 Chesterbrook Court, Apartment C, Indianapolis, Indiana, 46240. At approximately 9:30 a.m., Stewart left his apartment and drove to the nearby Carlyle Court Apartments, located at 951 Carlyle Lane, Indianapolis, Indiana, 46240 at which time he parked his car and opened a laptop. A few minutes later, Stewart closed his laptop and left the vicinity. Surveillance on Stewart was maintained throughout the day.

30. At the direction of the UNSUB over the course of several email communication, the Medical Excess company representative was directed to be at his office on the evening of September 30, 2008, at approximately 7:30 p.m. to await a phone call detailing directions for an extortion payment drop of \$10,000 in United States currency, in large bills.

31. On September 29, 2008, SA Odom photographed and recorded the serial numbers of \$10,000 in United States currency, in one hundred dollar bills. SA Odom then placed the currency in a brown paper bag and it was later provided to the company representative for use as the extortion payment.

32. On September 29, 2008, SA Odom received a telephone call from the Medical Excess company representative stating that he received a strange call on his office land line. The caller stated he was Federal Agent Jim Smith and that he was calling regarding the voice mail the

company representative left for him. The representative stated he did not know what the caller was referring to. The caller stated he was referring to tonight and the representative again stated he did not know what the caller was referring to. The caller then disconnected the call.

33. On September 30, 2008, at approximately 7:30 p.m., the company representative, accompanied by Mike Ward, Director of Investigations with the Indiana Attorney General's office, were at the Medical Excess office awaiting the call. At 7:36 p.m. the company representative received a phone call from the UNSUB who sounded as if he/she was using a voice altering device which made the voice sound computerized and female. The UNSUB directed the company representative to drive to the Huntington Bank at 91st and Meridian Streets and park in the parking lot and await further instructions.

34. On September 30, 2008 at approximately 7:39 p.m., surveillance observed Stewart leave his apartment 9133 Chesterbrook Court, Apartment C, Indianapolis, Indiana, 46240 and drive to Faith Missionary Church, 9125 North College, Indianapolis, Indiana, where he circled the parking lot twice. He then drove to the College Courts of Nora apartment complex, located on the north side of Faith Missionary Church, where at approximately 7:45 p.m. he parked in the vicinity of 9270 Yale Drive.

35. At 8:01 p.m., the company representative received a second call from the UNSUB using a voice altering device. The UNSUB asked the company representative if he was using air support, to which the company representative responded no. The UNSUB told the company representative to stay on the phone with him/her for directions. He/she advised the company representative to drive east on 91st Street, go through the stop sign to the stop light, to go through the stop light and take the first left into a church parking lot. This was Faith Missionary Church, 9125 North College, Indianapolis, Indiana. The UNSUB advised the company representative to

drop the money next to a white van on the northwest corner of the church parking lot. The company representative dropped the bag, containing \$10,000 in U.S. currency, as directed and then drove away.

36. At approximately 8:09 p.m. the company representative received another phone call, again with the voice altering device, (the caller sounded slightly out of breath) stating that the person had received a phone call stating that the package had been picked up and that the company representative would receive an e-mail in 12 hours from "the boss" advising that all was well and that the package had been received. The company representative acknowledged that the package had been picked up.

37. At approximately 8:14 p.m. surveillance observed Stewart departing the College Courts of Nora parking lot, turning northbound on College Avenue, then turned westbound on 96th Street. Surveillance was then lost on Stewart.

38. At approximately 8:45 p.m., Task Force Officer Rick Dean confirmed that the bag of money was no longer at the drop site location.

39. At approximately 9:08 p.m., surveillance observed Stewart returning to his residence at 9133 Chesterbrook Court, Indianapolis, Indiana 46204.

40. FBI Group Supervisor Tom White confirmed with SA Robert Herzog that Stewart's vehicle was parked at Yale Drive in advance of the drop. SA Herzog used Google Earth to determine that the distance between Stewart's car and the drop site was approximately one tenth of a mile.

41. On October 1, 2008, a Federal Search Warrant was executed at 9133 Chesterbrook Court, Apartment C, Indianapolis, Indiana, 46240 and numerous items were seized.

42. Among the items seized was a stack of one hundred dollar bills totaling \$10,000 in United States Currency. SA Herzog compared the serial numbers from the one hundred dollar bills that were seized from Stewart's residence with the serial numbers of the one hundred dollar bills SA Odom had placed in the brown bag for the extortion payment and confirmed that the serial numbers matched.

43. Also among the items seized was a Tracfone with a voice-altering device. Analysis of the call history of the cell phone revealed that a call was made to the Medical Excess office at approximately 4:08 p.m. on Tuesday, September 29, 2008. The call history also revealed a call made on September 29, 2008 at approximately 8:09 p.m. to cellular telephone number (317) 507-8736, which was the phone used by the company representative to await a phone call from the UNSUB.

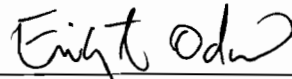
44. A Western Union receipt, under the name Jeff Hearld, was recovered in the glove box of Stewart's 2004 red Chevrolet Cavalier.

45. A blue zippered sweatshirt with a round logo consistent with the 2006 Medical Excess burglary video was also recovered from Stewart's apartment.

CONCLUSION

46. Based upon the information above, the Affiant believes there is probably cause to believe that Kevin M. Stewart has committed crimes in violation of Title 18 U.S.C. § 875 and Title 18 U.S.C. § 1030(a)(7)(B) and (7)(C).

FURTHER YOUR AFFIANT SAITH NOT



Emily A. Odom
Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me the 1st day of October, 2008.



Kennard P. Foster
United States Magistrate Judge
Southern District of Indiana